Medij. istraž. (god. 18, br. 2) 2012. (21-32)
STRUČNI RAD
UDK: 0040.7
Zaprimljeno: rujna 2012.

Lost in a Cloud: Overview of Legal Obstacles to the Growth of Cloud Computing

Gregory Graham*

SUMMARY

Cloud computing has emerged as an exciting new opportunity for smaller and mid-sized businesses to compete with larger companies. By increasing the utility of a company's computing ability without increasing maintenance cost, cloud computing has also given rise to a new industry: the provision of cloud services. The continued growth of an industry that is expected to be worth $216 billion could be hampered by legal obstacles. While cloud computing presents novel challenges to private international law, the single most obstructive issue facing the industry today is the European Union's policy towards data protection. Left unchanged, this policy could slow the growth of cloud computing at a time when IT industries need innovation. This piece provides an overview of what cloud computing is, the problems it poses for private international law, and then addresses the European Union's method to data protection regulation within the cloud.

Key Words: Cloud Computing, Cloud Service Provider, IT Industry, EU

Data Protection Directive

Introduction

The rise of cloud computing has begun to transform media technology and wider industries. No longer constrained by the relative size of their server network or budget limitations, businesses are taking advantage of cloud computing's prom-

* Gregory Graham, J.D. Candidate, May 2013, University of Pittsburgh School of Law, USA; gpg3@pitt.edu

ise to access previously unimaginable computing resources. Already profitable, the public cloud computing industry is expected to grow to $109 billion by the end of 2012.[1] This technological revolution is occurring around the world, and Croatia is no exception.

As the global market for cloud services grows, action taken towards improving cloud services in Croatia will improve a stagnating Croatian IT industry.[2] This movement has already begun to take place: Altus IT, based in Zagreb, has selected IBM PureSystems to transform its operations into that of a cloud service provider. (Rubsamen (2012)). Monolith Advertising, an Estonian-Croatian company, has realized the benefits of adopting Windows Azure as its platform to continue to grow its interactive advertising business. (Lange (2012)). Croatian Telecom specifically targeted its cloud services towards small and mid-sized businesses to take advantage of the burgeoning market.[3] These examples are only the beginning, and as Croatia moves into the European Union the potential for opportunities within the cloud will only grow.

Hand-in-hand with promises of more effective computing ability comes legal uncertainty due to the fundamental premise of the service: the data can be simultaneously uploaded, processed, and accessed anywhere. (Greco (2012)). If the data exists everywhere and is not located at a specific geographic point, whose law applies? Whose courts have jurisdiction? In response to this increase in worldwide usage, legal systems must adapt their rules concerning private international law to the legal questions posed by cloud computing or risk standing as an obstacle to international commerce.

Furthermore, due to Croatia's approaching accession date, EU regulations regarding Data Protection and the exercise of judicial jurisdiction over non-EU defendants create a substantial problem for the growth of the cloud computing industry. This paper briefly examines the legal issues created by the rise of cloud computing. Part I introduces cloud computing and highlights potential problems across legal systems while Part II specifically demonstrates that the European Union's approach to Data Protection within the cloud creates problems for the largest providers of cloud services: those based in the United States. The resulting uncertainties currently stand as barriers to the continued innovation and development of cloud computing as an industry.

I – Cloud Computing and Private International Law

Modern businesses run on applications.[4] SAP, Oracle, and Microsoft all offer applications and software designed for business efficiency. That efficiency comes at a cost, as all computer-based applications require a data center with accompanying office space. This data center requires servers, networks, and staff to maintain and update all of this equipment and software. The equipment needs cooling systems and a network staff to conduct development, to carry out testing, and to constantly monitor the system. As a business grows, so does the financial cost of development, use, and maintenance of necessary applications. Smaller companies find it hard to develop an extensive network in order to expand their business because the costs required act as an industry restriction. Due to this, small business organizations fail in competition with bigger companies, which possess the means of affording the equipment required to expand their business.

Taking advantage of infinite storage space and fast delivery, cloud computing has emerged as a desirable method for small and large businesses to efficiently run needed applications at low costs.[5] Instead of paying for the application, maintenance, and storage themselves, businesses turn to cloud providers over the Internet and pay a subscription for those applications to be accessible anywhere and at any time. Although cloud computing comes in numerous forms and can be both industry-wide or customer-specific[6], only the three most basic forms are needed to introduce and discuss the implications for private international law.

Infrastructure as a Service

Commonly referred to as the "base layer", Infrastructure as a service ("Iaas") serves as the foundation for cloud computing. All infrastructure required by a business - including servers, routers, firewalls, data storage and utility, and other network equipment is provided by the IaaS provider. As an example, with Amazon Elastic Compute Cloud (Amazon EC2) clients pay either by the hour or a flat rate for usage of the server capacity.[7] The customer is free to modify the amount of service provided.

Platform as a Service

As an intermediate level between basic infrastructure and highly specialized software, Platform as a Service ("PaaS") is a variation in which the purchasing company uses a third-party web provider's infrastructure to create or upload their own

materials that are in turn used to create individual applications. Applications for mobile devices are often constructed on this type of data-sharing platform. The provider will deliver the platform on the web, and in most cases customers can work on the platform using their own browsers. There is no need to download any software. This combination of simplicity and cost efficiency empowers small and mid-size companies, or even individual developers, to launch their own cloud software services. Google App Engine and Microsoft Windows Azure are both examples of platform services.[8]

Software as a Service

Software as a Service ("SaaS") is the most specialized form of cloud computing and consists of web based services, typically a software package or individual program. These packages are then used in specific divisions of a company, such as human resources. A company would then purchase a number of packages to fit their business model. New employees are given access to download the required programs through various devices, and on-site costs for network and server maintenance are reduced. On the customer side, it means no upfront investment in servers or software licensing; on the provider side, with just one app to maintain, costs are low compared to conventional hosting. Salesforce, a SaaS provider, provides sales software for Burberry, NBC Universal, and Tommy Bahama.[9]

Cloud Computing and Private International Law

In order to understand why cloud computing poses a challenge for private international law, it is necessary to first define and distinguish the concepts of jurisdiction and applicable law.[10] Applicable law is the substantive law that will govern a proceeding or dispute. In order for a court to hear a dispute, it must have adequate grounds for an exercise in jurisdiction over both the subjects and the subject matter involved and it must also have some law, or method of choosing the appropriate law, to apply to the rights and obligations of the parties involved.

Jurisdiction can be thought of in three basic conceptualizations. *Legislative* or *prescriptive* jurisdiction is when a legislature or governing body passes laws to prescribe conduct. (Symeonides, 2008: 23) *Adjudicatory* or *judicial* jurisdiction is when a court or other authoritative organ applies those prescribed laws to resolve a dispute concerning individual parties. (Symeonides, 2008: 23) Finally, *enforcement* jurisdiction is the authority to enforce those laws when they are not complied with. (Symeonides, 2008: 23) Jurisdictional authority has traditionally found justification

within the territoriality principle, which holds that a State may rightfully regulate the events in, and persons present within, their territory. (Symeonides, 2008: 23) From the principle of territoriality, the evolution of extraterritorial jurisdiction and "the effects doctrine" arose. (Symeonides, 2008: 23) Both extraterritorial jurisdiction and the effects test are potentially implicated when a state is concerned with actors outside its borders acting in such ways that would cause effects within them. (Trachtman (1998)) Legislative jurisdiction refers to prescribing conduct outside a State's borders; the following example may be instructive.

When Country A passes laws regulating who can enter into a contract, or what terms are deemed unenforceable in that contract, the country is exercising its prescriptive jurisdictional authority. If a court in Country A is hearing a dispute between two parties, that court is exercising its adjudicative jurisdiction. And if that court, through a contractual provision the parties agreed to, applies the law prescribed by Country A, that law will be the applicable law to the dispute. Seemingly straightforward, this example becomes more difficult if Country A originally passed a law that, in effect, regulated conduct outside its borders. Or if the court in Country A heard a dispute involving parties from Country B and C who, due to the broad scope of Country A's law, were found to be in violation of it.

While these challenges are not novel, cloud computing introduces an additional wrinkle. If a PaaS provider is using the infrastructure of an IaaS provider to provide services to an SaaS company creating a software program for a specific client, the application of a certain law or the exercise of adjudicatory jurisdiction becomes much more complicated. Cloud users don‘t necessarily know in which data centers or even countries their data is stored, or which sub-providers are being used by the provider with whom they have a direct relationship. Indeed, even cloud service providers who use other providers‘ resources (e.g. a SaaS service layered on IaaS or PaaS) may not necessarily know which data centers or countries are implicated in their business arrangements. As a result, a state prescribing rules as to how the personal or financial data of its citizens is stored or processed may now be indirectly prescribing rules for people who have no contacts with that state.

While there are a limited number of special laws and provisions of jurisdiction for Internet activities, the general rule is that the method of doing business is subject to the same basic rules and principles as other business methods that have an international or multijurisdictional element to them. (Stern (2011)) Each relevant state thus has its own private international law rules and principles[11], not all of which deal expressly with web-based activities. Cloud computing providers, and companies using cloud computing, could be confronted with multiple jurisdic-

tions whose laws governing the protection and availability of data are significantly different from their own. Uncertainties about which jurisdiction's law applies, or which State has personal jurisdiction may dissuade individuals and businesses from engaging in electronic commerce, can be disturbing to individuals whose personal data are processed, and may place burdens on regulators.

II – European Union Data Protection and Cloud Computing

While the discussion above existed in theory, the European Union's adaptation of its Data Protection law to the cloud computing industry has posed a significant real-word risk to the development of the medium. As Croatia is scheduled to join the European Union on July 13th, 2012, the context in which the cloud computing industry has the potential to grow, and the limitations placed on it by harmful European Union approaches to data protection regulation, should be examined.

An analysis of the European Union's approach towards cloud computing must take into account both the controlling data protection law that regulates the conduct of cloud providers, and the adjudicatory jurisdictional rules that might limit where they could be brought to court should they violate that law. Unfortunately for non-EU based cloud service providers, the reach of the EU's data protection law is extensive. When coupled with plaintiff-friendly national rules for determining adjudicatory jurisdiction over non-EU defendants, the potential liability for US-based cloud providers is troublesome.

Data Protection Directive

There are questions of extraterritoriality associated with any regulation of globally accessible data. The stronger the requirement for compliance with the particular laws of one state, the more troubling the extraterritorial reach of that state becomes. The European Union's 1995 Data Protection Directive extends its regulatory framework far beyond the European Union's territorial boundaries. As it currently stands, and will stand under the 2012 proposed Data Protection Regulation[12], non-EU based cloud providers with the smallest contact with the European Union are subject to its nationally implemented data protection laws.

The European Union's Data Protection Directive was proposed in 1995. (Directive) Designed to help facilitate the free flow of information, goods, and capital around the common market (Directive: Preamble Sec. 3) – thereby increasing commerce – the Data Protection Directive lays out a regulatory framework for the processing

and transfer of data that member states must implement at the national level. The central provisions to this framework are laid out in Article 4(1):

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself. (Directive: art. 4(1)) As this analysis focuses on the application to non-EU based cloud providers, article 4(1)(c) is of paramount importance. As the language of article 4(1)(c) indicates, a "controller" is subject to the implemented provisions of the Directive if it "makes use of equipment, automated, or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." (Directive: art. 4(1)(c)) A controller is considered any person or legal entity who" determines the purposes and means of the processing of personal data." (Directive: art. 2(d)) Personal data is "any information relating to an identified or identifiable natural person (‚data subject'). " (Directive: art. 2(1)) Processing of that data includes "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, [or] use…." (Directive: art. 2(b)) As broad as these definitions are, equipment is defined even more broadly. According to the Article 29 Working Party, comprised of EU regulators, the definition of equipment supports a broad interpretation of a notion more along the lines of 'means', to include even surveys or questionnaires, or Internet cookies.[13]

This interpretation when applied to stacking IaaS, PaaS, and SaaS services creates a large degree of uncertainty. Cloud users don't necessarily know in which data

centers or even countries their data is stored, or which third-party sub-providers the party they themselves are receiving services from is using. As discussed in Part I, cloud service providers who use other providers‘ resources (e.g. a SaaS service layered on IaaS or PaaS) often do not know which data centers or countries are implicated in their business arrangements.

Suppose that in 2014, following Croatia’s accession to the EU, a US corporation with a handful of Croatian employees in New York uses a software service from a US SaaS cloud provider to process employee productivity. Due to the size of the corporation, that SaaS provider turns to an IaaS or PaaS company to layer the capabilities. Unknown to the US corporation and the SaaS provider, that IaaS or PaaS cloud provider has multiple servers in a data center in Germany. In that case, the US corporation is using equipment in the EU, so EU data protection law may apply to that processing - even if the data analysis was initially targeted to US residents and was collected in the United States. All of this would occur without the business being aware that they were under restrictions regarding disclosure and data export. (Directive: art. 7) The Directive also requires member states to establish local Data Protection Authorities (“DPAs”), which are government agencies dedicated to privacy and the administration of data protection laws. (Directive: art. 28) Given a broad grant of power to investigate, intervene, and bring legal action – they are still subject to a provision found in Article 22. Article 22 states that Member States must still provide “for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.” (Directive: art. 22) Cloud service providers such as the SaaS company in the previous example could then face two legal actions. The first from the national data protection authority pursuant to Article 28, and the second a private action from any individual harmed pursuant to Article 22.

Adjudicatory Jurisdiction

The two parties in the previous example are safe from the reach of the European Union as the only concern they have so far is an application of European Union *prescriptive* jurisdiction. However, as the European Union’s rules for exercising *adjudicatory* jurisdiction over non-EU defendants are also extensive, both those companies could potentially face suit in a European Union court.

A discussion of European Union jurisdictional rules as they are applied to commercial matters must begin with the Brussels I Regulation.[14] Under Brussels I, defendants domiciled in a Member State can be sued in the courts of that Member

State for claims arising anywhere. (Brussels I: art. 2) A few examples of specific jurisdiction can be found in matters of tort and contract. Article 5(3) provides that for "matters related to tort", defendants domiciled in a Member State can be sued in the courts where the harmful events occurred or may occur. (Brussels I: art. 5(3)) Similarly, for contractual disputes, Article 5(1) permits the plaintiff to bring suit in the courts "for the place of performance of the obligation in question." (Brussels I: art. 5(1)) The explicit rules in Brussels I[15], apply only to defendants domiciled in Member States of the European Union. (Brussels I: art. 4) Article 4 provides that if a defendant is not domiciled in a Member State, "the jurisdiction of the courts of each Member State shall . . . be determined by the law of that Member State." Therefore, appropriate jurisdiction for civil liability over a cloud service provider from the United States would be determined by the jurisdictional rules of the EU nation in which the plaintiff chooses to bring suit, not any rule laid out in Brussels I. As a result, a non-Member State domiciled cloud provider would have to account for potentially different jurisdictional rules for each country within the European Union.

Pursuant to the right to a judicial remedy found in Article 22 of the Data Protection Directive, any cloud provider could be brought before the majority of European courts on the basis of a violation of the nationally implemented directive. As civil law countries, including Croatia, generally recognize that for actions relating to tort, adjudicative jurisdiction is provided for both where the harmful acts occurred and where damage was suffered[16], a cloud service provider who unknowingly processes data and therefore violates the Data Protection Directive, simultaneously unknowingly creates jurisdiction in many European member courts.

Conclusion

Under the 2012 proposed Data Protection Regulation[17], the penalties imposed upon companies for these violations can range from *a mere* 250,000 Euros to up to 2% of their yearly turnover. (Foster (2012)) While this is daunting to a small SaaS provider who wishes to take advantage of layering to grow the business, it is outrageous for larger business as well. Although ultimately not fined, Google's anticipated fines under the new model during a recent dispute with a data protection authority would have been 758 million Euros. (Espiner (2012)) As the fines are so high, and the likelihood of providing cloud services without being in some violation of the Directive is so low, the likely outcome is that cloud computing will not grow as quickly nor innovate as rapidly as it could. Ultimately, the European

Union's approach to data protection generally, and the implications that means for cloud computing, have created a scenario where the initial policy for the Data Protection Directive are being defeated by its application. In addition to having a negative impact upon the potential recovery and growth of the Croatian IT industry, the dangers for stalling growth across all media technologies and industries is startling. As a result, the future of cloud computing appears murky. While still a powerful medium for unlocking business potential due to its benefits, the uncertainty surrounding its application to European markets will substantially slow its growth.

ENDNOTES

1 PTI. (09-18-2012)*"Public cloud computing market likely to grow 19.6% this year: Gartner"*, http://articles.economictimes.indiatimes.com/2012-09-18/news/33926226_1_cloud-services-iaas-market-services-market, date of access: Oct 20th, 2012.

2 The Croatian IT market declined 0.5% year on year in U.S. dollar terms to $1.15 billion in 2011. Measured in local currency, the market was down 3.3% from the previous year. IDC expects the IT market in Croatia to decrease 0.4% year on year in 2012 and then to grow at a compound annual growth rate (CAGR) of 6.0% to reach $1.53 billion in 2016. Croatian IT spending per capita stood at $255 in 2011, or 27% of the EU27 average of $956. Juras, I. (09-26-2012) "*Croatian IT Market Continues to Stagnate*", http://www.idc-cema.com/?showproduct=50541, date of access: Oct 17th 2012.

3 I.T. Footprint customer information, http://www.itfootprint.co.uk/Datacentres/1438714/calling_up_to_the_cloud.html, date of access: Oct. 10th, 2012; Vasco – Croatian Telecom case study, http://www.combis.hr/attachments/524_croatian_telecom.pdf, date of access: Oct. 1, 2012.

4 Put simply, a business application is any process or program a business uses to run more efficiently. Business applications can range from industry-wide offered services, such as SAP AG provided software, to specialized tools specifically designed for a small business. Consider applications to include any of the following: store-bought commercial products, internally developed systems, customized third-party provided systems, and processes that run on either client computers or servers.

5 A Microsoft survey of small business owners found that 44% believe that cloud computing makes them more competitive. 53% of those polled believed the switch to cloud computing services would improve sales volume. Edge Strategies, (02-08-2012), "*Drivers & Inhibitors to Cloud Adoption for Small and Midsize Businesses,* http://www.microsoft.com/en-us/news/presskits/telecom/docs/smbcloud.pdf, date of access: Feb 8th, 2012).

6 For a distinction between industry-wide "public clouds" and customer-specific "private clouds" *see* Hanson, K. (04-05-2012) *"Virtual Private Cloud Computing vs. Public Cloud Computing"*, http://cloudcomputing.sys-con.com/node/2230961, date of access: Oct 20th, 2012.

7 Amazon EC2 customer information, http://aws.amazon.com/ec2/, date of access: Oct 12th, 2012.

8 Google App Engine customer information, https://developers.google.com/appengine/, date of access: Oct 12th, 2012; Microsoft Windows Azure customer information, http://www.windowsazure.com/en-us/home/features/overview/, date of access: Oct 12th, 2012.

9 List of Salesforce Customers, http://www.salesforce.com/customers/, date of access: March 22nd, 2012.

10 The recognition and enforcement of judgments is not covered in this paper.

11 *See* Michaels, R. (2006) "Two Paradigms of Jurisdiction", Michigan Journal International Law, Ann Arbor, 27, 1003.

[12] The 2012 proposed Data Protection Regulation does not materially alter the application of European Union data protection laws to non-EU based cloud providers. Therefore the national implementations discussed in this paper and to be researched this summer will still highlight the means for US companies to limit their exposure to EU jurisdiction.

[13] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", WP 179 (2010). Cookies are text files that automatically save onto a user's computer via the user's Internet browser. Cookies are automatically read by the Internet browser during visits to that Website from then on. They can contain information regarding Internet preferences, online shopping, or surfing history.

[14] Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, (EC) No. 44/2001, 2000 O.J. (L012) [hereinafter Brussels I].

[15] This will change under the proposals for Revision of the Brussels 1 Regulation. Under the proposals, the jurisdictional rules of the Brussels Regulation would apply uniformly to all defendants in European Courts, including those from non-member states. Brand, R. (2011) *Fundamentals of International Business Transactions*. Pittsburgh: University of Pittsburgh.

[16] *See* Organic Law on the Judicial Power 1985 ('LOPJ'), Article 22(2) (LOPJ 1985, 6); Zivilprozessordnung § 13, 17, 32 (FRG); New Code of Civil Procedure Tl 3, Ch 2, art. 42, 43, 46 (France) ; L'Union des Etudiants Juifs de France v Yahoo Inc, Tribunal de grande instance [TGI] Paris, 12 April 2000, No 00/05308 (asserting jurisdiction on the basis that the defendant's conduct, even if occurred outside France, had caused effects in France); Swedish CJP, supran 167, Ch 10, s 8; Art 53(1) of the Croatian PIL Act.

[17] The proposed 2012 Regulation would uniformly toughen every requirement under the already existing Data Protection Directive. *See generally* Foster S., (02-09-2012), *"The EU Has Proposed a New Framework for Data Protection: What does this mean for your business?,* http://www.mintz.com/newsletter/2012/Advisories/1632-0212-NAT-PRIV/index.htm, date of access: Oct 12th, 2012). The proposal for a new regulation can be found here: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Izgubljeni u oblaku: Pregled pravnih prepreka razvitku računalstva u oblaku

SAŽETAK

Računalstvo u oblaku nastalo je kao uzbudljiva nova prilika da se manjim poduzećima i poduzećima srednje veličine omogući natjecanje s velikim kompanijama. Povećanjem korisnosti računalske sposobnosti neke kompanije, bez povećanja troška održavanja, računalstvo u oblaku također je potaknulo razvoj nove industrije: službe u oblaku. Kontinuirani rast industrije za koju se procjenjuje da vrijedi 216 bilijuna američkih dolara mogao bi biti otežan zbog zakonskih prepreka. Dok računalstvo u oblaku pretstavlja nove izazove međunarodnom privatnom pravu, problem koji najviše stvara opstrukcije u industriji danas jest politika Europske unije prema zaštiti podataka. Ostavljena nepromijenjena, ta bi politika mogla usporiti rast računalstva u oblaku u vrijeme kad je IT industrijama potrebna inovacija. Ovaj rad pruža pregled pitanja što računalstvo u oblaku jest, problem koji ono predstavlja međunarodno privatnom pravu te se osvrće na metode Europske Unije u zaštiti podataka unutar oblaka.

Ključne riječi: računalstvo u oblaku, uslužne službe u oblaku, IT industrija, Europska unija